REMARKS

The application has been amended in a manner believed to place it in condition for allowance at the time of the next Official Action.

Amendments to the Disclosure

Independent claim 10, dependent claims 11-14, independent claim 15, independent claim 20, dependent claims 21-22, and dependent claims 24-25, are amended to recite the invention in a manner more consistent with PCT/JP2005/001524.

The claims are further amended as to style in consideration of U.S. practice and preferences. These amendments to the claims are not believed to introduce new matter.

Independent claim 10, dependent claims 11-14, independent claim 15, independent claim 20, dependent claims 11-15, 21-22, and 24-25, remain pending.

Dependent claims 16-19 have been canceled without prejudice.

Formal Matters - Objections to the Claims

The Official Action objected to claim 10, stating that on line 32 of claim 10, the word --or-- needs to be added after the semi-colon and before condition (d) since the four conditions are written in the alternative.

In response, claim 10 is amended in a manner believed to overcome the Official Action's objection.

The Official Action objected to claims 15-19, stating that on line 1 of claims 15-19, for consistency, the word "tracking" needs to be replaced by --detection--.

In response, claim 15 is amended based on the claim recited on PCT/JP2005/001524 and defines the technical feature of "A network attack tracking system" to overcome the Official Action's objection. Additionally, claims 16-19 are canceled as indicated above.

The Official Action objected to claim 20, stating that on line 29 of claim 20, the comma after the word "progress" needs to be changed to a --semi-colon (;)-- to be followed by the word --or-- instead of "and" since the four conditions are written in the alternative; additionally, there's a missing colon (:) after the word "satisfied" on line 10; and conditions a-b also need to end with a semi-colon in place of a comma.

In response, claim 20 is amended in a manner believed to overcome the Official Action's objection.

The Official Action objected to claims 10 and 20, stating that since the four conditions of claims 10 and 20 are

written in the alternative, all variables should be defined within each condition or prior to all the conditions.

In response, claims 10 and 20 are amended based on the content pointed out to overcome the Official Action's objection.

Based on the amendments to the claims and the remarks provided above, withdrawal of all the objections is respectfully requested.

Rejection of claims 10 and 20 under Section 112

Claims 10 and 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. In particular, the Official Action asserts that four conditions recited in claim 10 and claim 20 are written in the alternative.

The Official Action states that each condition is understood to be able to stand on its own, and yet condition (c) is written to depend on (b), and therefore the Official Action states that the claim is unclear or indefinite.

The Official Action also asserts that the limitation "coefficient computed in (b)" is claims 10 and 20 has insufficient antecedent basis because there is no "coefficient" mentioned in (b).

In response, claims 10 and 20 have been amended to overcome the Official Action's rejections for indefiniteness. The Applicants submit that no new matter is believed to have been added by the amendment of the claims.

Withdrawal of the rejections under 35 U.S.C. 112, second paragraph is thereby respectfully requested.

Rejection of claims 10-19 under Section 101

The Official Action rejected claims 10-19 under 35 U.S.C. 101, stating that the claimed invention is directed to non-statutory subject matter. In particular, the Official Action asserts that the claims are directed to program/software per se.

In response, the claims have been amended to further recite "processors programmed to perform" the recited steps. Support for the amendment may be found, for example, in Figure 1 disclosing a communication monitor processor 4 performing the software steps that the individual processors take. It is respectfully submitted that no new matter is believed to have been added.

Based on these amendments, it is believed that the claims 10-19 have been placed into compliance with 35 U.S.C. 101. Withdrawal of this rejection under Section 101 is respectfully requested.

Rejection of claims 10-19, 20-22, and 24-25 under Section 103

The Official Action rejected claims 13-14 and 24-25 under 35 U.S.C. 103(a) as being unpatentable over Chesla et al. (US 2004/0250124; hereinafter "CHESLA") in view of Apap et al. (US 7,448,084; hereinafter "APAP").

The Official Action rejected claims 10-12, 15-17 and 20-22 under 35 U.S.C. 103(a) as being unpatentable over CHESLA in view of APAP, and further in view of Chao et al. (US 7,526,807; hereinafter "CHAO").

The Official Action rejected claims 18-19 under 35 U.S.C. 103(a) as being unpatentable over CHESLA in view of APAP as applied to claims 13 and 14 above, and further in view of CHAO.

The rejections are respectfully traversed for the reasons provided below.

The Official Action offers CHESLA as teaching a network attack detection system, wherein it is judged that an illegal attack has taken place by observing the values of the packet header fields, based on paragraph [0023] of this reference. However, the Official Action concedes that CHESLA fails to teach that when a number of distinct values seen in a combination of two or more header fields exceeds a pre- specified threshold value within a pre-specified time, an attack is judged to be in progress.

The Official Action contends that APAP discloses that statistics gathered in observing how many distinct values occur in a monitored feature and compared against a model of normal usage in a registry access system can be used in detecting malicious activity (column 12, lines 51-60).

The Official Action asserts that it would have been have been obvious to a person having ordinary skill in the art at the time the invention was made to modify CHESLA and incorporate APAP to meet the preceding limitation not explicitly disclosed by CHESLA.

At this point, a brief review of the applied references is believed to be helpful.

CHESLA discloses a method for protecting a network from an attack, comprising the step of statistical analysis to develop one or more signatures of packets participating in the attack (such as values of one or more packet header fields), determining at least one parameter characteristic of the participating traffic, and filtering the traffic by blocking traffic characterized by the parameter. The determining step includes counting occurrences of packets characterized by each of the plurality of parameters in the traffic and determining the number of occurrences occurred within a certain period time.

APAP discloses a method for detecting intrusions in the operation of a computer system, comprising the step of analyzing features (consisting of a name of a process, a type of a query,

an outcome of a query, a name of a key, and a value of a key) from a record of a process that accesses the operating system registry. A check is performed to determine if a value of the feature has been previously observed for the feature, a score is computed if the value of the feature has not been observed, and the access is labeled as anomalous if the score is greater than a predetermined threshold.

In contrast, the invention as recited in the independent claims 10 and 20 judges an unauthorized attack based on “the number of distinct values” observed in the pre-specified fields in the packet header. That is, one of the judgment indicators of independent claims 10 and 20 is “the number of distinct values”, (for example “the number of distinct values” of source address field, or port number field, or destination address field, etc.).

This is not disclosed in either CHESLA or APAP.

Especially, APAP's approach is different from that of the claimed invention because:

APAP: for an access

a. detects value of feature which comprises of the values of "consisting of a name of a process, a type of a query, an outcome of a query, a name of a key, and a value of a key"

b. computes a score for the feature value

c. based on the score decides whether the access is anomalous.

In the present invention: for an access

a. compute the number of feature values

b. based on the number of feature values we decide whether the access is a attack.

For example, in a case where distinct source addresses S_1, S_2, $\cdots$,S_N are observed in the source address field of the M packets ($M \geqq N$) seen within a pre-specified time interval, "the number of distinct values" is N. In a case where "the number of distinct values" of source address field increases, it is judged that an unauthorized attack (for example, a DDos attack) may be in progress.

CHAO discloses determining packets to be described in response to a DDos attack using the equation that is computed by comparing currently measured attribute values to nominal attribute values, and using various thresholds and combinations thereof.

In contrast, independent claims 10 and 20 recite judgment of an unauthorized attack by computing the ratio of "the number of distinct values" to other numbers (described in conditions (a)-(d)), and determining whether the ratio reaches the pre-specified threshold. That is, the judgment point of independent claims 10 and 20 is to use the ratio of "the number of distinct values" to other numbers, instead of the number of values. This feature is not disclosed in either CHESLA or APAP.

As a further example, in a case where the number of packets and “the number of distinct values” of source address field are observed within a pre-specified time interval (e.g., 16:00-16:30 as shown in the chart presented below), it is judged that an unauthorized attack (for example, a DDos attack) may be in progress within the time 16:20-16:25 because the ratio of “the number of distinct values” to number of packets has been seen to increase within the time 16:20-16:25.

Time	The number of packets	The number of distinct values
16:00-16:05	3,500	20
16:05-16:10	5,000	25
16:10-16:15	65,000	325
16:15-16:20	7,500	40
16:20-16:25	4,000	170
16:25-16:30	4,500	22

Therefore, the accuracy of detecting an unauthorized attack will be increased independently of the increase and/or decrease of the number of packets due to using the ratio of “the number of distinct values” to other numbers. Thus, this will avoid a faulty judgment in case the traffic fluctuates widely and randomly in a network with a web server.

As clarified above, independent claims 10 and 20 have a remarkable and unexpected effect not present in either of CHESLA’s disclosure or APAP’s disclosure, and it would not have been obvious to a person having ordinary skill in the art at the

time the invention was made to modify CHESLA to incorporate APAP and CHAO.

It is therefore respectfully submitted that independent claims 10 and 20 are patentable over CHESLA and APAP.

The claims respectively depending from claims 10 and 20 are also believed to be patentable at least for depending from patentable parent claims, and additionally for the following reasons.

Dependent claims 11 and 21 recite judgment of an unauthorized attack based on “the number of distinct values” observed in the arbitrary combinations of two or more fields in the packet header. This also is not disclosed in either APAP or CHAO.

For example, in a case where “the number of distinct values” of source address field and port number field are observed, an unauthorized attack will be judged according to the application classification. Thus, an unauthorized attack such as a minor DDos attack with few changes in the number of addresses will be detected independently of the increase and/or decrease in the number of packets.

Dependent claim 11 in combination with independent claim 10 and dependent claim 21 in combination with independent claim 20 have a remarkable and unexpected effect of increasing

the accuracy of detecting an unauthorized attack. This effect does not exist in either of APAP's disclosure or CHAO's disclosure.

Dependent claims 12 and 22 recite judgment of an unauthorized attack based on the TTL value in addition to "the number of distinct values" observed in the packet header fields; this also is not disclosed in APAP and CHAO. Dependent claim 12 in combination with independent claim 10, and also dependent claim 22 in combination with independent claim 20, have a remarkable and unexpected effect of increasing the accuracy of detecting an unauthorized attack. This effect does not exist in either of APAP's disclosure or CHAO's disclosure.

Dependent claims 13 and 24 recite judgment of an unauthorized attack based on "the number of distinct values" observed in the arbitrary combinations of two or more fields in the packet header. That is, one of the judgment indicators of dependent claims 13 and 24 is "the number of distinct values" (for example "the number of distinct values" of source address field, or port number field, or destination address field, etc.). This is not disclosed in either APAP or CHESLA.

For example, in a case where distinct source address S_1, S_2, $\cdots$,S_N are observed in the source address field of the M

packets (M ≧ N)seen within a pre-specified time interval, “the number of distinct values” is N. In a case where “the number of distinct values” of source address field and port number field are observed, an unauthorized attack will be judged according to application classification. Thus, an unauthorized attack such as a minor DDos attack with few changes in the number of addresses will be detected independent of the increase and/or decrease in the number of packets. This effect is not taught or suggested in either of APAP’s disclosure or CHAO’s disclosure.

Also, dependent claims 14 and 25 recite judgment of an unauthorized attack based on the TTL value in addition to “the number of distinct values” observed in the packet header fields. This feature is not disclosed in either APAP or CHESLA. Dependent claim 14 in combination with independent claim 13, and dependent claim 25 in combination with independent claim 24, have a remarkable and unexpected effect of increasing the accuracy of detecting an unauthorized attack. This effect is not taught or suggested in either of APAP’s disclosure or CHAO’s disclosure.

Claims 15-19 recite a step to determine the source address of an unauthorized attack by using the network attack detection system described in claims 10-14. This also is not disclosed in either APAP or CHESLA. Dependent claims 15-19 have

a remarkable and unexpected effect of increasing the accuracy of searching the source address of an unauthorized attack. This effect does not exist in either of APAP's disclosure or CHAO's disclosure.

Based at least on the reasons set forth above, Applicant respectfully requests withdrawal of the rejections of the claims under Section 103.

Conclusion

From the foregoing, it will be apparent that Applicant has fully responded to the December 21, 2010 Official Action and that the claims as presented are patentable. In view of this, Applicant respectfully requests reconsideration of the claims, as presented, and their early passage to issue.

In order to expedite the prosecution of this case, the Examiner is invited to telephone the attorney for Applicant at the number provided below if the Examiner is of the opinion that further discussion of this case would be helpful in advancing prosecution.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

/Jeremy G. Mereness/

Jeremy G. Mereness, Reg. No. 63,422
209 Madison Street
Suite 500
Alexandria, VA 22314
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

JGM/jlw